Electronic Trespass in Canada: The Protection of Private Property on the Internet.

James Macdonald.

I. Introduction.

It is perhaps trite to observe that the rapid growth of the Internet has led to the development of a dynamic body of law loosely referred to as Internet law or cyberlaw. Issues that a decade ago would have baffled the majority of lawyers and academics — "e-commerce patents, e-commerce law, trademark and domain name conflicts, online copyright infringement, jurisdiction in cyberspace, and web site liability for defamation"[1] — are now firmly established areas of the law, ripe for litigation and academic discourse. The development of Internet law has not been even across all disciplines, however; while intellectual property is seen as synonymous with Internet law, tort law has for the most part been left behind.[2] The Supreme Court of Canada has ruled on the relationship of intellectual property to the Internet,[3] but no court in Canada has considered the availability of private property rights such as trespass to chattels.[4] As a result, important questions over the application of property rights to the Internet have remained unanswered.

Canadian courts need not start from scratch when formulating a Canadian approach to Internet property issues. Just as tort law lags behind intellectual property law, Canada lags behind the United States in Internet jurisprudence. While this may be a source of frustration for Canadian lawyers, the result is that Canadian courts have the benefit of almost a decade of litigation in the United States concerning the protection of property rights on the Internet. The source of this American jurisprudence is the resurrection of the "late, largely unlamented tort of trespass to chattels" as the tort of electronic trespass.[5] Part II of this paper traces the development of electronic trespass in the United States, from the initial application of trespass to chattels to telephone communications to the creation of the doctrine of electronic trespass to deal with spam, web robots, and spyware.

This paper argues that Canadian courts can, and should, adopt electronic trespass as a viable cause of action for the protection of property rights on the Internet. Of course, this conclusion presupposes that property rights in fact exist on the Internet. While American courts have accepted the existence of property rights on the Internet without any real controversy, a significant body of criticism has developed around American jurisprudence. Part III examines the critiques levelled against the assumption of property rights inherent in electronic trespass, and argues that there are property rights that need to be protected on the Internet. Part IV addresses the practical issue of whether electronic trespass is available at common law in Canada. Focusing on the tangible quality of electronic communications and the lack of requirement to show actual damages, this paper concludes that electronic trespass is a viable cause of action in Canada. Despite being a viable cause of action, Part V examines the concerns of the anticommons movement, and considers whether Canadian courts should forgo electronic trespass and adopt an alternative doctrine resembling nuisance. In rejecting such an approach, this paper concludes with a discussion of the importance of consent as a means of imposing rationality on the operation of electronic trespass, and questions the usefulness of legislative reform.

II. Electronic Trespass in the United States

Creation of Electronic Trespass: *Thrifty-Tel.*

The starting point for the development of electronic trespass in the United States was the California Court of Appeal's judgment in *Thrifty-Tel, Inc. v. Bezenek*.[6] While the case did not deal with the issue of trespass over the Internet, it is important because the court held for the first time that electronic signals were "sufficiently tangible to support a trespass cause of action".

The defendants in *Thrifty-Tel* were involved in what was popularly known as "phreaking": exploiting

telephone networks by technological means to obtain free services. Using a confidential access code, the defendants used a modem to connect to the plaintiff telephone carrier's telephone network. Once they gained access to the network, the defendants ran manual and automated searches for the authorization codes required to access the plaintiff's automated switching network, which in turn allowed the defendants to make free long distance calls. While the manual searches had an apparently negligible impact on the plaintiff's system, the automatic searches "overburdened the system", preventing other users from accessing the system.[8]

The plaintiff succeeded at trial on the basis of conversion in the unauthorized use of the confidential codes. On appeal, however, the court noted that conversion actions were not traditionally allowed if they only related to "intangible interests that are not merged with, or reflected in, something tangible".[9] The court did not fully consider this issue, since it held that the evidence was sufficient to support an action based on the "seldom employed" tort of trespass to chattel.[10] An action could be made in trespass to chattel "where an intentional interference with the possession of personal property has proximately caused injury".[11] Quoting Prosser's characterization of trespass to chattels as the "little brother of conversion", the court emphasized the tort's applicability to situations where personal property was merely used without authorization.[12]

In *Thrifty-Tel*, the court had little difficulty concluding on the evidence that the defendants' actions were intentional, that the plaintiff had a possessory interest in the telephone network, and that the defendants' actions likely damaged the telephone network.[13] As stated above, the court also found that an action in trespass to chattels could be based on the electronic signals sent from the defendants' modem over the plaintiff's telephone network. The court held that the original requirement in trespass of direct physical contact had been expanded to allow for indirect contact. Further, the court held that the "requirement of a tangible has been relaxed almost to the point of being discarded",[14] noting that other courts had already based actions in trespass on microscopic particles, smoke, and sound waves.[15] With this relatively brief legal analysis — entirely contained within a single footnote — the court established the legal basis for parties to enforce their property rights on the Internet.

Electronic Trespass and Spam: *CompuServe*.

As even the most casual user of e-mail is well aware, spam is "unsolicited commercial e-mail" that clogs the inboxes of Internet users.[16] In 2004, spam accounted for as much as 80% of global e-mail traffic, lowering efficiency and trust in the Internet, and acting as a "direct threat to the viability of the Internet as an effective means of communication".[17] In response to the growing spectre of spam (and perhaps the lack of effective legislative approaches),[18] Internet Service Providers (ISPs) in the United States successfully used *Thrifty-Tel* to find liability for spammers based on the tort of electronic trespass.[19]

In *CompuServe, Inc. v. Cyber Promotions, Inc.*[20] the plaintiff ISP sought a preliminary injunction based on trespass to chattels to stop the defendants from sending spam to its customers over its network. The court relied on the *Restatement (Second) of Torts* for its formulation of the proper test: "a trespass to chattel may be committed by intentionally using or intermeddling with the chattel in possession of another".[21] Following *Thrifty-Tel*, the court held that electronic signals were sufficiently tangible to support a trespass action.[22]

The court concluded that the defendants' actions diminished the value of the plaintiff's network, even though the defendants did not physically damage the network.[23] The plaintiff only had to show a "diminution of [the server's] quality, condition or value"; to hold otherwise would blur the distinction between conversion and trespass to chattels.[24] The affidavit evidence of CompuServe technicians stated that storing and processing spam placed a "tremendous burden on [CompuServe's] equipment".[25] While the court did not discuss how much of this burden was specifically the result of the defendant, it was satisfied that "to the extent that defendants' multitudinous electronic mailings demand the disk space and drain the processing power of plaintiff's computer equipment", the defendant's actions reduced the resources that CompuServe could supply its subscribers, which in turn diminished the value the plaintiff could derive from its computer equipment.[26] The court further noted that the defendants' actions resulted in customer complaints and cancellations, which harmed CompuServe's "business reputation and goodwill with its customers".[27]

Electronic Trespass and Robots: *eBay* and *Ticketmaster*.

In the wake of the successful application of electronic trespass to spam, established Internet corporations successfully widened the application of electronic trespass to include communications between commercial parties over the Internet in a series of cases concerned with the use of robots. Robots, also known as spiders, Web bots, or Web crawlers, are software agents: code designed to automate the actions of human users. The most significant use of robots, though by no means the sole use, is to "crawl" the Internet to populate search engine databases. In this capacity, robots are essential to the practical operation of the Internet. Google's database, for instance, contains information on literally billions of Web pages; a database this size simply could not be created, let alone maintained, in any efficient manner by human agents. Jeffrey Rosenfeld offers this helpfully succinct definition

of a robot/spider and the technological process involved in crawling:

> [A] spider is a program that automatically traverses the Web's hypertext structure by retrieving a document, and recursively retrieving all documents that are referenced. A spider visits a Web page, reads it, and then follows links to other pages within the site. This is what it means when someone refers to a site being "spidered" or "crawled".[28]

The language in the above definition needs some clarification: the use of terms such as "traverse"and "crawl" gives the impression that the robot somehow inhabits the target server. In reality, the robot only operates as software on the originating server, sending out multiple requests to the target server.[29]

In admittedly broad terms, robots are used to access the contents of Web sites for one of two reasons: (1) to create a value-added product that does not directly compete with the target Web site; or (2) to directly compete with the target Web site.[30] Examples of the former include the Googlebot or MSNBot; both robots attempt to compile a comprehensive listing of publicly accessible content on the Internet. The generally positive impact of these robots on the Internet is rightly lauded.[31] While these robots are for the most part created with a commercial purpose, they do not compete directly with the Web sites they crawl. Indeed, in the majority of cases it will benefit the owner to have his or her Web site crawled by these robots so the content can be found by potential users.[32]These beneficial robots (to date) have not provoked electronic trespass litigation.[33] The second type of robot, however, is not particularly beneficial to the party whose server is being crawled.[34] These robots are programmed to access a specific server, usually in an attempt to copy the contents of a competitor's Web site.

A robot's activities were first held actionable in electronic trespass by a California district court in *eBay, Inc. v. Bidder's Edge, Inc.*[35] The defendant, Bidder's Edge, ran an auction aggregation Web site: instead of hosting auctions, the defendant's Web site provided users with listings from multiple third-party auction sites. The defendant used a robot to crawl third-party auction sites, including eBay.com, to populate its database. The defendant was initially given verbal approval to crawl the plaintiff's Web site while the two parties negotiated a licensing agreement. When the negotiations ended without success, the plaintiff requested that the defendant stop including information about eBay auctions on its Web site. While the defendant initially complied with the plaintiff's request, it continued to use a robot to crawl eBay's servers, despite additional unsuccessful negotiations, and despite further notices from the plaintiff that its activities were unauthorized. In response to the continued crawling of its Web site by the defendant, the plaintiff attempted to block the Bidder's Edge robot through technological means. The technological response proved largely ineffective, however; the robot ignored eBay's Robot Exclusion Standard,[36] and used proxy servers to circumvent eBay's attempts to block known IP addresses used by the robot.[37]

Adopting the Supreme Court of California's reasons in *Thrifty-Tel*, the court outlined the test for trespass to chattels over the Internet as follows:

> In order to prevail on a claim for trespass based on accessing a computer system, the plaintiff must establish:
>
> (1) defendant intentionally and without authorization interfered with plaintiff's possessory interest in the computer system; and
>
> (2) defendant's unauthorized use proximately resulted in damage to plaintiff.[38]

In applying this test to the present facts, the court largely followed the rationale used by the courts in *CompuServe* and subsequent spam cases.

The defendant argued that it did not access the plaintiff's Web site without authorization because the Web site was freely accessible to the public. While the court elsewhere questioned the appropriateness of comparing the passage of the defendant's robot through the plaintiff's network to a physical intrusion into a "brick and mortar" store,[39] the court stated that the plaintiff's network was private property, to which the public is only given "conditional access".[40] When the defendant crawled the Web site despite repeated requests from the plaintiff to desist, the defendant exceeded the scope of the plaintiff's consent. The defendant was likewise unsuccessful in its argument that it did not interfere with the plaintiff's possessory interest in the network. The defendant argued that the plaintiff was required to prove a substantial interference with its possessory interest, which was not evident on the facts. While the court agreed that the plaintiff would likely be unable to prove that there was a substantial interference, the court went on to hold that while there was "some uncertainty as to the precise level of possessory interference required to constitute an intermeddling", the plaintiff was only required to show that the defendant had "use of another's personal property".[41]

In assessing whether the plaintiff would be able to prove actual damages, the court adopted the formulation of damages used in *CompuServe*: "A trespasser is liable when the trespass diminishes the condition, quality or value of personal property".[42] The defendant testified that it sent 80,000 to 100,000 requests per day over the plaintiff's network. While this number may at first seem impressive, the defendant's actions accounted for at most 1.1% of the data transferred over the plaintiff's network.[43] The plaintiff did not, however, claim any specific damage above the use of its network.[44] Nonetheless, the court held that this level of activity was likely sufficient to find real damage:

> Even if, as [Bidder's Edge] argues, its searches use only a small amount of eBay's computer system capacity, [Bidder's Edge] has nonetheless deprived eBay of the ability to use that portion of its personal property for its own purposes.

> The law recognizes no such right to use another's personal property.[45]

Further, the court held that if it did not find that the defendant's use constituted an injury to the plaintiff, "it would likely encourage other auction aggregators to crawl the eBay site, potentially to the point of denying effective access to eBay's customers".[46]

American commentators have criticized the decision in *eBay* for being too expansive in its application of electronic trespass. Maureen O'Rourke expressed the general consensus among critics when she argued that *eBay* created "a broad rule that would allow a site to obtain an injunction against all unwanted visitors", a property right that is broader than exists in real property law (where intangible interferences are dealt with through a balanced approach in nuisance), and trespass to chattels (where the duration and size of the interference can limit liability).[47] In the face of this concern over the unchecked growth of electronic trespass, however, the availability of the tort was restricted in the first reported decision to consider *eBay*.

In *Ticketmaster Corp. v. Tickets.com, Inc.*,[48] the defendant ran a Web site that included information on tickets offered for sale on the plaintiff's Web site, as well as links to the specific pages on the plaintiff's Web site where users could purchase tickets. As in *eBay*, the information from the plaintiff's Web site was collected with a robot. The defendant did not receive any money from users who purchased tickets from the plaintiff, but presumably benefited from increased traffic due to more comprehensive listings. There was no contractual relationship between the parties, and the plaintiff took technological measures to prevent the links from the defendant's Web site from working properly.[49] The plaintiff brought a motion seeking a preliminary injunction to prevent the defendant from crawling the plaintiff's network. The court denied the plaintiff's request for a preliminary injunction. However, despite professing to follow *eBay*, the court's reasoning in *Ticketmaster* was at odds with the prior decision.

The court noted that the burden the defendant's robot placed on the plaintiff's network "appears very small and there is no showing that the use interferes to any extent with the regular business of [the plaintiff]. If it did, an injunction might well issue…".[50] Further, the court did not believe that denying the injunction would likely result in other parties crawling the plaintiff's Web site to the point that its business would suffer. The court even reasoned that the defendant's activities were likely beneficial to the plaintiff, as it possibly resulted in increased ticket sales. The court failed to take into account *eBay*'s position that any loss of processing power was sufficient for the establishment of damages; *Ticketmaster*, in effect, established a minimum level of interference that was absent from *eBay*. Post-*Ticketmaster* courts, however, largely abandoned the requirement that the plaintiff show a minimum level of interference.

In *Register.com, Inc. v. Verio, Inc.*,[51] the plaintiff domain name registrar brought a preliminary motion to prevent the defendant from crawling its WHOIS database[52] to collect information on registrants for marketing purposes. In granting the plaintiff's motion, the court adopted the lower standard established in *eBay*.[53] While the plaintiff was unable to provide any direct measurement of the system resources tied up by the defendant's robot[54] (and the court did not cite any evidence that the plaintiff's network actually had suffered from the defendant's actions), the court reaffirmed that mere use, even if negligible, was sufficient to constitute an interference with a possessory interest. The court also accepted the plaintiff's "floodgate" argument — that allowing the defendant to continue to crawl its network would encourage other parties to do the same — but it considered this in connection with the irreparable harm factor of the test for receiving an injunction, not for whether the plaintiff was likely to succeed on the merits of its claim.

The minimum level of interference required in *Ticketmaster* was explicitly rejected in *Oyster Software, Inc. v. Forms Processing, Inc.*[55] In this case, the defendant used a robot to copy metatags from the plaintiff's Web site to improve its search engine rankings.[56] The plaintiff brought an action against the defendant for, among other things, trespass to chattels. The defendant brought a motion for summary judgment on the trespass claim, arguing that its robot did not compromise "the basic function" of the plaintiff's network. Indeed, on the plaintiff's own evidence the defendant's actions had a negligible effect on its network. In considering what level of interference was required, the court concluded that *Ticketmaster* had incorrectly interpreted *eBay*; the plaintiff had a valid claim in trespass "not because the interference was 'substantial' but simply because the defendant's conduct amounted to 'use' of" the plaintiff's network.[57] This requirement that the plaintiff merely show "use" was even less onerous than in *eBay*, where the plaintiff had to show some damage flowing form the interference.

Limiting Electronic Trespass: *Intel*.

The California Supreme Court cast doubt on the correctness of the *eBay* approach in *Intel Corp. v. Hamidi*,[58] the current leading case on electronic trespass. Over the course of 21 months, Hamidi, a disgruntled former employee of the plaintiff, sent six "mass e-mails" to Intel employees via their Intel e-mail addresses.[59] The e-mails generally criticized Intel's business and employment practices, and urged employees to join an advocacy group formed by Hamidi. Despite the absence of evidence that Hamidi's e-mails impaired the functioning of Intel's computer network,[60] Intel received a permanent injunction enjoining Hamidi "from sending unsolicited e-mail to addresses on Intel's computer systems" on the basis of trespass to chattels.[61] The California Court of

Appeal upheld the lower court decision, stating that trespass to chattels without any proof of actual damage to personal property was actionable because Hamidi "was disrupting [Intel's] business by using its property".[62] In a thorough review of the relevant case law, the California Supreme Court reversed the decision of the California Court of Appeal.

The court held that in order to succeed on a trespass action involving electronic contact, the defendant's actions had to cause "some actual or threatened interference with the computers' functioning".[63] In the opinion of the court, *eBay* should not be read, as it was in *Oyster Software*, as only requiring the "use" of the plaintiff's network.[64] Instead, *eBay* and subsequent cases showed that the court would grant an interlocutory injunction when the interference was negligible only if denying the claim would encourage others to use the plaintiff's network in a manner that would substantially interfere with the network's function.[65] Thus, the court did not grant an injunction in *Ticketmaster* because the defendant's actions were negligible *and* there was no threat of others overburdening the plaintiff's network in a similar manner.[66] In the present case, the e-mails used only a negligible portion of the plaintiff's network.[67] Intel's complaints were concerned solely with the content of the e-mail. In the opinion of the court, "those interests are protected by other branches of tort law; in order to address them, we need not create a fiction of injury to the communication system".[68]

Those who hoped the court would maintain the lower standard set in *eBay* unsurprisingly took a negative view of the decision:

> Despite Intel's demands that he stop, and its efforts at self-help, Hamidi persisted in intruding where he was not welcome. Intel posted a "Private Property, Keep Out" sign, but Hamidi refused to comply, and the California Supreme Court refuses to honor it.[69]

However, for critics of *eBay*, the decision in *Intel* was welcome because it "anchored" trespass to chattels "to its traditional foundation as a means for defending possession in personal chattels. . .".[70] While the decision in *Intel* has received a mixed reaction, most commentators agree that its practical effect was to limit the broad application of electronic trespass established in *eBay*.[71]

Patricia Bellia argues that *Intel* not only limits the application of *eBay*, but also undermines the very basis for electronic trespass established in *CompuServe*.[72] The core of Bellia's reasoning is that the damage accepted in *CompuServe* was the same type of damage rejected in *Intel*. In both cases, the networks could easily accommodate the increase in traffic; the e-mails caused damage because of their content (i.e., customers in *CompuServe* and employees in *Intel* having to deal with unwanted messages). Thus, plaintiffs after *Intel* will have to show a significant interference with their networks to succeed.[73] This argument is not entirely satisfying. While the content of the e-mails in *CompuServe* may have made for a sympathetic court, the legal analysis adopted in the *CompuServe* line of cases did not depend on the commercial nature of the e-mails. CompuServe's network was central to its business. The defendants' actions limited CompuServe's ability to use its network, leading to customer dissatisfaction. It was not legally relevant whether the interference came in the form of spam or some other activity such as a robot, as long as a portion of the network was used without consent. However, *Intel* does likely mean that mere use as advocated by *Oyster Software* is not enough. Given the court's specific comparison to the level of harm experienced by ISPs in the spam cases to Hamidi's actions, *Intel* has raised the harm requirement in electronic trespass cases dealing with e-mail. In effect, *Intel* has limited the applicability of *CompuServe* to spam, or at the very least to non-commercial e-mails sent in volumes indicative of spam.

George Fibbe argues that the impact of *Intel* will be minimal, stating that *Intel* "is a poor vehicle for assessing the interests of Web site owners against commercially harmful scrapers".[74] While Hamidi's actions may have annoyed Intel, they were unlikely to cause actual economic harm. Hamidi's interference with the network did not "compromise any core aspect of [Intel's] business",[75] as opposed to robot cases where the interference directly affets the plaintiff's ability to provide services to other users. As such, Intel was unable to show the irreparable harm that was required for an injunction. Further, Intel failed to satisfy its self-help obligation by not directing employees to request that their names be removed from Hamidi's mailing list; by contrast, in robot cases, the plaintiff rarely has the opportunity to take effective self-help measures.[76]

The Future of Electronic Trespass: *Sotelo*.

Although there have not been any reported post-*Intel* e-mail or robot cases, an Illinois district court recently applied electronic trespass to spyware. In *Sotelo v. Directrevenue, LLC, et al.*,[77] the court allowed the plaintiff to proceed with a claim in trespass against the defendants for allegedly installing spyware surreptitiously on the plaintiff's computer. The defendants argued that since the plaintiff could close every pop-up advertisement as it appeared, there could not be any actual damage. The court held that this argument ignored "the reality of computer and Internet use. . .".[78] In its conception of the potential damages that could be claimed by the plaintiff, the court included "wasted time, computer security breaches, lost productivity, and additional burdens on the computer's memory and display capabilities".[79] This list of injuries is consistent with *eBay*, as it either relates specifically to the capacity of the plaintiff's computer, or to time spent by the plaintiff servicing his computer in relation to the defendant's actions.[80] The recognition that electronic trespass is equally applicable to an individual user's personal computers as it is to a corporation's server farm has the potential to encourage a diversity of cases based in trespass to chattels.[81] One can hope that

viewing the legal rationale behind electronic trespass through varied factual situations will help settle questions related to the required level of harm in the United States.[82]

III. Do Property Rights Exist on the Internet?

The question of whether or not electronic trespass can succeed in Canada is, at its core, a debate over the appropriate role, or even existence, of property on the Internet. Holding that a party can enforce private property rights arising from electronic communications necessarily presupposes that there is a property right that can be enforced. Unsurprisingly, this is not something all commentators are ready to concede. Indeed, critics of electronic trespass are wary about the imposition of property norms on the Internet, warning that it "threatens the very foundations of the web".[83] This concern is primarily advanced through the argument that electronic trespass gives property rights reserved for chattels to intangible objects.

Does Electronic Trespass Give Property Rights to an Intangible Object?

American courts have consistently concluded with little difficulty, or even discussion, that computer networks are property for the purposes of trespass to chattels. Laura Quilter criticizes this assumption as obscuring fundamental questions about the nature of property on the Internet: "While computers are undoubtedly chattels, it is questionable whether electronic networks and computer processing power also qualify as chattel."[84] In a similar manner, Daniel Hunter questions the willingness of courts to apply property rights to intangible things such as bandwidth and processing power: "With the exception of the computer itself, none of these 'chattels' are actually chattels at all. There is no private property in bandwidth or processing power or network."[85] While it is likely correct that an owner does not have a property interest in something as ephemeral as processing power, the above critiques mischaracterize the property interests protected by electronic trespass.

The hardware making up the network in an electronic trespass case can be identified as a chattel without any controversy: the hard drives, memory boards, computer racks, among other hardware items, are all tangible objects that possess an identifiable value.[86] If an agent of Bidder's Edge walked off with eBay's physical servers, eBay would have a straightforward action in conversion. However, as the court noted in *eBay*, it is not clear if eBay could make a similar claim if Bidder's Edge somehow stole its bandwidth.[87] Applying trespass to chattels to this example, it is logical to conclude that eBay should not be able to sustain an action in trespass for interference with bandwidth; bandwidth, as an intangible thing, cannot sustain damage as contemplated by property law.[88] Thus, Wendy Adams argues that in order for actions in electronic trespass to be successful, courts rely on a legal fiction that transforms "processing activity into an object of property rights".[89]

The difficulty with the above critique is that electronic trespass does not protect the property interest of intangible things such as bandwidth and processing power in and of themselves. Rather, electronic trespass considers these things as intangible attributes of the physical hardware. When the court in *CompuServe* held that the interference diminished the server's processing power, it was not protecting the processing power, but rather, relying on the diminished processing power as proof of the interference to the server. Consider by analogy the effect of an interference with a possessory interest in a car. The main attribute of the car, the reason the car has value to its owner (in a utilitarian sense, at least), is motion. If the owner is prevented from using the car due to an interference from another party — i.e., if he or she is unable to use the car to move — the owner will have an action in trespass to chattels against the other party. The court would not give much credence to the other party's argument that his or her actions only interfered with the movement of the car, which as something intangible cannot be the subject of property rights. The right of the owner to use the car free from interference is exactly what is protected from trespass. Similarly, the main functional attribute of a server is its processing power. If someone interfered with the server in a way that restricted the owner's ability to use the server's processing power, the owner has a claim in trespass based on interference to the server, not the processing power. Adams states: "There is an object, the server, and there is activity, the processing of requests, but the activity and the object are not one and the same."[90] While critics of electronic trespass are wary of using place metaphors such as "cyberplace" when describing the Internet,[91] they continue to rely on metaphor to the extent that they separate the activity of the Internet from its physical reality. Under this conception, the activity of the server is something more than a mere function of the physical hardware: it is a legal space that exists separately from the physical hardware that produces the activity. In effect, focusing on the activity of the server as the legal object severs property rights from a chattel (the server) just because the chattel has a primarily intangible function.

A less theoretical criticism is that, while ostensibly about the protection of chattels, electronic trespass is really about the protection of information: the Web site may just be a function of the server, but it is the Web site that is actually being protected by electronic trespass. To quote a rather caustic passage from a decision in *Ticketmaster*:

> [Deleting the claim in trespass to chattels] should hurt no one's policy feelings; after all, what is being attempted is to apply a medieval common law concept in an entirely

> new situation which should be disposed of by modern law designed to protect intellectual property interests.[92]

Indeed, electronic trespass cases tend to involve situations where the action in question threatened the protection of commercial data.[93] Electronic trespass allowed eBay to stop a competitor from crawling its database without having to resort to copyright law. However, criticizing electronic trespass because it may intersect with intellectual property rights unduly limits the scope of Internet law to purely intellectual property matters. As discussed above, electronic trespass can arise in situations that have nothing to do with the protection of copyright, such as spam or spyware. More importantly, the right to exclude is a fundamental power given to the possessor of a chattel in property law,[94] and is not dependent on the possessor's reasons. Once it is established that there is a property right to protect, courts do not differentiate between a reasonable attempt to exclude and an unreasonable one.[95] Instead of rejecting electronic trespass on policy grounds because it can be used to shield intellectual property from competitors, concerns over the protection of intellectual property through property law should be dealt with through existing antitrust or intellectual property legislation.

IV. Is Electronic Trespass Actionable in Canada?

While trespass to chattels has been revived in the United States, it still languishes in relative obscurity in Canada. Having discussed whether property rights even exist on the Internet, it is useful now to examine whether these property rights can be protected at common law in Canada by the tort of electronic trespass.

Despite the paucity of case law,[96] the following definition represents the general consensus among Canadian authorities: trespass to chattels is actionable "where the defendant directly and intentionally (or negligently) interferes with a chattel in the possession of the plaintiff".[97] While the elements of the tort in Canada are similar to the requirements in the United States, there are two possible differences in the tort's potential application. The first difference concerns the tangible quality of electronic signals — i.e., could *Thrifty-Tel* be followed in Canada? While courts in the United States have found that electrons are sufficiently tangible for actions in trespass, it is not clear that a Canadian court would come to a similar conclusion. The second difference concerns the likely absence of the need to show actual damage at common law in Canada, removing a substantial stumbling block faced in the American actions.

Can One Trespass with an Electron?

In *Thrifty-Tel*, the court considered for the first time whether electronic signals were sufficiently tangible to sustain a claim in trespass to chattels in California. In holding that the electronic signals were sufficient, the court relied on previously recognized actions in trespass to land based on microscopic particles, smoke, and sound waves.[98] The acceptance of an action over electronic signals was essential for the creation of electronic trespass. A Canadian court faced with the facts in *Thrifty-Tel* would likewise find an absence of any prior authority extending intangible incursions to trespass to chattels. However, a Canadian court would not have any significant prior authority allowing a trespass to land based on an intangible excursion.

The volume of case law supporting the extension of trespass to intangible incursions is minimal. The Court of Appeal of Ontario in *Bower v. Richardson Construction Co. Ltd.*[99] allowed damage to an adjoining property caused by vibrations emanating from a steam pile driver to be compensated in trespass. In *McDonald et al. v. Associated Fuels Ltd. et al.*,[100] the British Columbia Supreme Court suggested in *obiter* that damage caused by carbon monoxide blown into a residence from an exhaust pipe could be actionable in trespass to land. These two rather antiquated cases have not been followed in subsequent decisions, and are at odds with the general treatment of intangible incursions in trespass law.[101] Instead of opening trespass up to intangible incursions, Canadian courts have persisted in holding that any action concerned with an intangible interference to a property interest, such as the movement of smoke or sound, is properly pleaded in nuisance.[102] This preference is seen in *Phillips v. California Standard Co.*[103] The defendant's "artificially generated seismic waves"[104] — used to search for oil deposits — coursed through the plaintiff's property, causing damage. While the plaintiff brought an action in trespass, the court held that the plaintiff's action was properly in nuisance: "trespass involves a physical entry on the property of another and in the case at bar that physical entry never took place".[105]Despite the usual practice of dealing with intangible incursions in nuisance, however, all is not lost for the potential plaintiff. The Canadian common law's general recognition of the importance of the protection of property rights and the need for legitimate compensation suggest that a Canadian court would likely allow an action in electronic trespass to proceed.

Clifton Merrell has criticized the holding in *Thrifty-Tel*, contending that "[e]lectrons seem entirely too ethereal and metaphysical to justify a cause of action at law".[106] Further, allowing trespass by electronic signals would lead to "absurd results", such as claims in trespass to "fax machine[s] [and] household appliances attached to an outlet".[107] Merrell's litigious dystopia, however, may not be as ridiculous as first imagined. It is admittedly difficult to think of situations where a person's possessory interest in a toaster would be subject to a temporary interference by means of electrons. Nonetheless, if an intentional power surge over the electricity grid caused the toaster to burst into flames, it would be counterintuitive to deny the owner of the burnt toaster a claim in

tort simply because the fire was caused by the movement of electrons, as opposed to a more tangible interference. The damage resulting from electronic trespass is not usually as obvious as a burning server farm; nonetheless, the lack of physical indicia by no means equals an absence of damage or interference.[108] Denying a claim because the interference was not obviously physical would conflict with the basic purpose of property torts at common law: the protection of an interest in a chattel.[109]

While the different categories of tort are theoretically organized based on the nature of the interference — i.e., conversion for permanent interference, trespass to chattels for transitory interference — the main focus is on the actual impact on the property. As even the sceptical court in *Ticketmaster* noted:

> The computer is a piece of tangible personal property. It is operated by mysterious electronic impulses which did not exist when the law of trespass to chattels was developed, but the principles should not be too different. If the electronic impulses can do damage to the computer or to its function in a comparable way to taking a hammer to a piece of machinery, then it is no stretch to recognize that damage as trespass to chattels and provide a legal remedy for it.[110]

The hardware that makes up the Internet has the same property interests as any other chattel. Courts should therefore not have to unduly stretch the common law to realize that a server could be severely damaged or curtailed by electronic signals.[111] Disallowing claims in electronic trespass based on the questionable tangibility of electronic signals would deny compensation for plaintiffs who have suffered real damage, an arbitrary result that would showcase the inability of the law to account for technological progress. Of course, property interests can still be protected under nuisance. However, as discussed below, nuisance is not the proper tort theory to protect property rights on the Internet.[112]

Is Actual Damage Required?

A particular fixation in the American case law concerns the requirement to show actual damage in trespass to chattels. Although no Canadian court has specifically addressed this issue, a plaintiff likely does not have to show actual damage to succeed on a claim in trespass to chattels in Canada. The *Canadian Encyclopedic Digest* summarizes the requirements for the tort as follows: "any unauthorized touching or moving of a chattel is actionable at the suit of the possessor, *even though no harm ensues*".[113] One of the few appellate-level discussions of trespass to chattels advances the opposite proposition. In *London Drugs Ltd. v. Kuehne & Nagel International Ltd.*, Southin J.A. at the B.C. Court of Appeal adopted the following definition from *Halsbury's Laws of England* in her dissent: "Trespass to goods is an unlawful disturbance of the possession of the goods by seizure or removal or by a direct act *causing damage to the goods*."[114] This statement is not particularly persuasive, however, as the question of whether damage was required was not at issue, and in any event the dissent was rejected on appeal.[115]

Lower courts have shown a willingness to allow actions in trespass to chattel without actual damage. In *Hudson's Bay Co. v. White*,[116] the defendant stole five pairs of gloves from the plaintiff department store. The defendant was apprehended by security, and the gloves were returned undamaged. The court held that trespass to chattels was actionable without damage. In the absence of proof of actual damage, however, only nominal damages would be available.[117] In *Burns v. Financial Bailiff Services Ltd.*,[118] the court held that the defendant bailiffs trespassed on the plaintiffs' van when they unlawfully entered the van with the intent to seize it. Since the plaintiffs "were never deprived of the use of the van … they suffered no actual damages",[119] and were thus unable to claim pecuniary damages. Despite the lack of actual damage, however, the claim in trespass to chattels was still used as an actionable wrong for the award of punitive damages. While the case law is not conclusive, it suggests that trespass to chattels is actionable *per se*.[120] An action in electronic trespass, the issue of tangibility aside, should therefore be easier to establish in Canada than in the United States.

V. Is Electronic Trespass the Best Way to Protect Property Interests?

Even if it is accepted that there are property interests on the Internet that need to be protected by property torts, it is not immediately obvious that this has to be done by trespass to chattels. A number of commentators have argued that the development of electronic trespass will lead to the "tragedy of the anticommons". In an attempt to protect the integrity of the Internet, these critics have called for the adoption of a cyber-nuisance regime that balances the interests of owners and users.[121] For supporters of electronic trespass, what the critics are calling for "is the equivalent of declaring open season on cyber property, giving uncompensated rights to all-comers for the use of a web site's limited resources".[122] This position is unnecessarily alarmist, as the cyber-nuisance regime does not allow for unrestricted access. Nonetheless, the creation of a cyber-nuisance regime would leave an identifiable species of chattel open to physical interference in a manner inconsistent with Canadian common law. The policy issues raised by critics of electronic trespass need not be brushed aside, however; the recognition of the importance of consent in the architecture of the Internet[123] will allow for the adoption of electronic trespass in a manner that ensures the continued beneficial development of the Internet.

Will Electronic Trespass Lead to the Tragedy of the Anticommons?

Whether or not property rights exist on the Internet, some commentators have argued (as mentioned above) that electronic trespass should not be supported because it will lead to the "tragedy of the anticommons": "no one will be allowed to access competitors' cyberspace 'assets' without either licensing access or agreeing to some other transactionally expensive permission mechanism", resulting in an "inefficient underuse" of resources.[124] Further, cordoning off the Internet into exclusive territories will lead to a decline in innovation[125] and free speech.[126] Daniel Kearney argues that the anticommons movement unrealistically sidelines the role of commerce in the present Internet, relying on a mythical conception of a borderless Internet: "The Internet did not arrive with a set of pre-existing legal entitlements."[127] In Kearney's conception of a market-driven Internet, commercial parties should be left to their own devices to come to agreements over how best to allocate resources.[128] In this sense, market forces alone will ensure that Web site providers keep the Internet open to an acceptable degree.[129] Additionally, other commentators argue that the dream of an open Internet is not realizable given even the current level of technological methods designed to block access.[130]

Whatever the conclusion to this argument, it needs to be recognized that this dispute is essentially academic and does not adequately account for the global nature of the Internet — the Internet has continued to grow unabated despite the rise of electronic trespass in the United States. And as is argued below, the cyber-nuisance regime supported by members of the anticommons movement is unsatisfying. Instead, the concerns of the anticommons movement can be met through a robust notion of implied consent.

Should Electronic Trespass Be Dealt with in Nuisance?

The creation of a doctrine of cyber-nuisance relies on the flexibility of nuisance law to balance competing interests.[131] Steven Kam argues that trespass to chattel's "harm-based analysis focuses on literal damages but asks few questions as to the worth of the trespassory activity".[132]Thus, using the balanced approach of nuisance, the court could properly contrast the competing worth of the defendant's speech in *Intel* with the defendant's commercial goals in *eBay*.[133]

The idea of using nuisance to deal with electronic interferences is not a novel idea in Canada. In *Motherwell v. Motherwell*,[134] the court held that a claim in nuisance was actionable for communications carried over the telephone system. Although it was the content and character of the communications that were actionable in *Motherwell*, rather than the communications themselves, it suggests that technological communications can carry the tort of nuisance in a manner that bridges the physical distance between a plaintiff and defendant. Despite this precedent, however, cyber-nuisance should not be adopted in favour of electronic trespass.

Nuisance is properly focused on protecting an occupier's proprietary interest in the use and enjoyment of his or her real property; Linden thus describes nuisance as an "environmental tort".[135] With the possible exception of claims brought by users whose home computers had been infected with spyware,[136] the connection to the plaintiff's real property is not evident in the electronic cases discussed above: where, for instance, is the proprietary interest in real property in *CompuServe*? The overburdened servers at the heart of this case were most likely not kept on the plaintiff's premises. It would be difficult to argue that the use of servers at an off-site server farm would somehow affect the use and enjoyment of a separate piece of real property.

The above argument, while attractive in its simplicity, is not wholly persuasive. Nuisance should not be rejected simply because it only applies to real property, and is therefore inapplicable to the Internet. Kam sensibly describes this objection as a mere "formalistic obstacle" that should not be used to prevent nuisance from grappling with the "problems of inherently communal cyberspace".[137] The problem with casting this objection aside, however, is that the focus on real property is not merely formalistic. The question that needs to be asked is whether nuisance can be extended to include the types of property interests at play on the Internet. It is on this basis that cyber-nuisance should be rejected. The balancing of interests in nuisance is a direct response to interactions unique to the use and enjoyment of real property and cannot easily extend to the operation of the Internet in a manner that adequately protects property rights.

The balancing of interests in nuisance is a recognition that real property does not exist in isolation, but is surrounded by other parcels of real property in a common environment:

> The ambition of nuisance law has never extended to providing every plaintiff with a serene hermitage, but has been limited to providing restrictions on the most intolerable or obnoxious of the unpleasant consequences of living in proximity to other members of society. In this respect the sanctity of any person's proprietary interests must be weighed against the competing interests put forward by others.[138]

As such, an occupier should reasonably expect that the effects of an action in a neighbouring property would necessarily flow into his or her real property. Since the occupier can be expected to have the use of his or her real property interfered with to a reasonable degree by a neighbour's actions, the neighbour's motives become relevant. The electronic trespass cases discussed above do not fit within the general purpose and concern of nuisance. The conception of the Internet as a common environment where information flows freely between indi-

vidual servers is at odds with the reality of an Internet made up of individual servers that can accept or reject communications deliberately sent from other servers. This is true even if, as a matter of course, individual servers accept incoming communications. The spam sent by the plaintiff in *CompuServe* was not the indirect overflow of electronic signals from the defendant's property; it was a direct incursion onto the plaintiff's network in a manner more consistent with trespass than nuisance.

Cyber-nuisance is premised on the idea that some level of interference with other servers should be allowed, regardless of whether the owner of the server consented to the interference. What is important is the purpose of the interference. Because the interference in *Intel* was worthwhile, under a cyber-nuisance regime Hamidi would be able to trespass on Intel's servers. Therefore, under cyber-nuisance owners have to accept a certain level of interference with their chattels, despite a legitimate property interest in the functionality of servers. This opens up a species of chattels to a level of interference that would be unacceptable with other chattels with more obviously physical functions. Supporters of cyber-nuisance would argue that, while there is no social utility in allowing parties to trespass on another's interest in physical chattels, there are strong reasons to allow interferences with property rights over the Internet. However, to the extent that these concerns are valid, they can be adequately accounted through a consideration of the role consent plays in the availability of electronic trespass.

Consent and Electronic Trespass.

The abandonment of cyber-nuisance as a viable alternative in favour of electronic trespass does not mean the common law will inevitably be used to protect the property interests of Web site owners to the ultimate detriment of the Internet and society. In advocating an "open Internet", Jennifer Granick, the executive director of the Stanford Law School Center for Internet and Society, states:

> The law should treat the Internet as open by default -- a public resource rather than a gated community. This doesn't mean that we can't protect our networked computers or data with copyright law, passwords, firewalls or perhaps even terms-of-service agreements. But rather than asking whether a user obtained permission to access computers connected to the Internet, the law should ask whether the owner did anything to prevent public access.[139]

Granick correctly highlights that impracticality of requiring express consent for every communication (and thus every use of other hardware) on the Internet.[140] It is not apparent, however, why this necessarily means the Internet needs to be treated as a public resource. Adams argues that the defence of consent will not have any practical effect in rationalizing the use of electronic trespass because plaintiffs will simply contact potential defendants and request that they stop accessing their server.[141] This is a curious objection, since it suggests that the Internet should operate on the basis of intractable or forced consent where, short of removing one's server from the network, one has to accept all incoming communications. Granick recognizes that system owners can legitimately take steps to prevent access, an action at odds with the concept of a public resource. The Internet Granick describes resembles private property that the public has an open invitation to use, such as commercial establishments. The Supreme Court of Canada has held that extending an open invitation to enter to the public does *not* give the public any general right of access.[142] Open access does not require the extinguishment of property rights.

Electronic trespass can operate within the framework of an open Internet as long as Canadian courts follow the American jurisprudence in its treatment of consent. In *CompuServe*, for instance, the court held that the plaintiff had given its tacit consent to use its server because anyone could send e-mails over its network. This consent was removed when it requested that the defendant not send spam over its network. Similarly, in *eBay* the court held that the plaintiff had given users of its system a conditional access; crawling the site was expressly restricted by the Web site's terms of use. By crawling eBay's Web site in the face of an explicit request to cease such activity, Bidder's Edge exceeded its consent. Thus, an action will only lie in electronic trespass if the plaintiff has withdrawn its consent, or the defendant has exceeded the plaintiff's consent.[143]

Consent or license is a full defence to an action in trespass. Therefore, if courts are going to enforce actions in trespass on the Internet, it is important to consider how the content of the consent or license will be determined. In cases where the parties have entered into a licensing agreement, it is relatively straightforward to determine what actions would exceed the scope of the license. Determining when consent has been exceeded or restricted is more difficult, but can be accomplished through the recognition of implied consent and the ability to expressly restrict consent.

The recognition of implied consent on the Internet is important because, in its absence, every electronic communication made without express consent would give rise to a claim in electronic trespass. Fortunately, the reality of the Internet's technological architecture suggests that the vast majority of electronic communications over the Internet take place on the basis of implied consent:

> [T]he most basic functions of the Internet — sharing wires and sending and receiving messages — would be impossible without the cooperation of every single machine connected to the global network. This cooperation, contrary to judicial assumptions, requires implied consent to outside use of bandwidth and processing power.[144]

Judicial recognition of the implied consent inherent in the Internet will allow electronic trespass to be applied

in a beneficial and reasonable manner. Thus, a user will not be trespassing for merely visiting a Web site — opening a Web site up to the Internet implies that other servers will use the network's resources. Indeed, technology issues aside, it is counterintuitive to hold that an owner has not given the public an invitation to use its resources when the owner has taken steps to connect his or her network to the Internet. Similarly, a user would not be trespassing with a robot if the user was not given any indication that his or her access was not permitted.

While it is easy to find implied consent in basic electronic communications — i.e., "visiting" a Web site — courts will have a more difficult time establishing the limits of implied consent on the Internet. Given the lack of any clear definition of the content of implied consent, it is tempting to call for the adoption of legislation to outline the type of behaviour electronic trespass is meant to catch. The benefit of legislation, in theory, is that if the scope of consent is set by legislation, then everyone can govern his or her actions accordingly. However, the risk of enacting legislation is that any list of acceptable behaviour will quickly become outdated. There is a significant lag time in the creation of legislation; any statute designed to respond to any specific technological problem may very well be outdated by the time it receives royal assent. Moreover, courts have already shown themselves able to adapt to changing standards of Internet behaviour in determining the scope of acceptable behaviour over the Internet. In *1267623 Ontario Inc. v. Nexx Online Inc.*[145] the court gave judicial approval of the concept of "netiquette" or Internet etiquette.[146] In this case, the court held that spamming was a breach of netiquette for the purposes of a contractual term between the spammer and an ISP. Netiquette can thus be used to remove the benefit of implied consent in situations where, for instance, spam is sent over a computer network, spyware is installed on a user's personal computer, or possibly even when a robot excessively crawls another server. Leaving the categories of behaviour open will allow courts to enforce property rights in situations where the defendant has acted badly and thus deserves sanction (especially important in the absence of any harm limitation at common law in Canada).

The implied consent discussed above can, of course, be expressly restricted. However, with the exception of clearly communicated restrictions between parties such as in *eBay*, it is not yet clear what steps need to be taken to effectively communicate the restriction. One possible way is through a Web site's terms of use, often called browserwrap agreements. In *CREA v. Sutton*,[147] the court let the plaintiff rely on its Web site's terms of use, despite the fact that it was never brought to the defendant's attention.[148]While the decision in *CREA* is relatively narrow — the defendant should have known there would have been a terms of use provision because it had a similar document on its own Web site — it suggests that in certain situations the scope of consent to use a network's resources can be outlined in the Web site's terms of use. Communication of express restrictions can also rely on netiquette. For instance, a restriction on consent can be communicated through commonly accepted technological protections. If a user has to circumvent security protections to access a network, or if the robot crawls a site in violation of the terms in the Robot Exclusion Standard, it is likely that he or she has breached the owner's implied consent.

By allowing the content of consent to be decided on a case-by-case basis, courts can develop a flexible notion of implied consent informed by notions of netiquette and common practices, and identify situations when the implied consent has been restricted. This will allow electronic trespass to be used to curtail less desirable activities, and support the use of technological means to prevent unwanted access[149] without unduly limiting the socially useful aspects of the Internet.

VI. Conclusion.

Without denying its revolutionary impact, the Internet is essentially just a series of interconnected chattels. Despite the use of monikers such as "cyberplace", the Internet is rooted in the physical world, and the transmission of electronic signals over the Internet can cause actual damage off-line. Richard Epstein interprets the debate over electronic trespass as dealing with "the hard question [of] whether technological changes could ever lead us to abandon the presumption that a deliberate trespass counts as a private wrong".[150] This paper suggests that the answer should be no. As a means to protect property rights in chattels, trespass to chattels has remained relatively consistent since the Middle Ages,[151] evidence of the common law's ability to accommodate technological change.[152] The Internet is changing the manner in which people relate to each other, but the common law need not be forced in radical new directions to deal with the inevitable problems that arise any time two or more people interact. A computer network is a chattel, holding the same property rights as any other tangible object; the mere act of connecting a computer network to another network should not automatically open up the network to unlimited interference, to the detriment of any possessory interests.